November 2015 Volume 1, Issue 2

Security Matters

SITSD
Enterprise Security Program

Security Matters is the monthly information security newsletter published by the Enterprise Security Program. Each month we also have a supplemental file of materials you can use for security awareness. You can find that file at: http://sitsd.mt.gov/Montana-Information-Security/Security-Training-Resources

We hope you'll find the newsletter and materials useful and hope you'll give us feedback on what we can do better. Your suggestions for topics and content are welcome. Contact us.

Focus on Mobile Devices

Not so long ago – although it's hard to remember those dark days – a phone was a how you called someone from across town or the country, a tablet was made of paper, and a mobile computing device weighed 10 pounds or more and was called a laptop. Phones, tablets, and laptops are all still part of our daily lives, but, boy, have they changed! And they've been joined by even more options for connecting and communicating. You can make phone calls, send text messages, watch television and movies, read books, do your banking, play games, shop for everything from clothes to groceries to a new car and even work from a device that fits in your pocket and weighs less than half a pound. There are apps for nearly everything you can imagine. These days most of us use a mobile device of one type or another and we'd feel a little lost without it (or them!). There's even a word for the fear of being without one's mobile phone: nomophobia.

All that functionality and power is incredibly useful, but it can also put you and your information at risk. Just like your computer at work and at home, you likely store, send, and receive emails, files, and pictures on your phone, tablet, and/or laptop. Without taking precautions, that information can often be stolen much easier than hacking into your home or business networks. You have a password or may even use two factor authentication for your computers, but are you doing the same for your mobile devices? Surveys say that 70% or more people don't password protect their phones.

Mobile devices are becoming attractive targets for malware and ransomware, too. While the thought of cleaning an infected phone might not sound too …

Continue on page 6

Mobile Device Management with Airwatch Enterprise Mobility Management

Mobile device technologies such as smartphones and tablets have fundamentally changed the ways State of Montana employees are conducting business. Recognizing that these devices change the risks to State of Montana resources as well as changes were needed to help agency staff manage all of the mobile devices that employees use conducting State business, SITSD and multiple agencies worked on creating a Mobile Device Management (MDM) RFP. That RFP was awarded and the AirWatch Enterprise Mobility Management (EMM) platform was purchased the spring of 2015 as a scalable EMM solution to securely get business-critical data, email, applications and content onto State of Montana employees' smartphones, tablets and computers. In addition, another critical aspect of the EMM product was that it provided ways to protect the employee's privacy on Bring Your Own Devices (BYOD).

From the start, the State of Montana AirWatch EMM solution was built by SITSD to provide core infrastructure functionality and enterprise wide security and privacy features while also providing a flexible environment for each agency to to test the functionality of the products and develop policies and procedures to effectively secure and

Continue on page 5

Inside this issue:

A monthly update on the latest security threats and other software news.

- Sean Rivera, CISSP

“Microsoft’s latest operating system release, Windows 10, brings some interesting features to security at the enterprise level that warrant a look. “

Windows 10 Security Enhancements

With each iteration of an operating system release users hope for a noticeable return on investment in the time it takes to install or migrate. When it comes to security, there are always improvements being introduced to operating systems. Microsoft’s latest operating system release, Windows 10, brings some interesting features to security at the enterprise level that warrant a look. Here is the breakdown of some of these features.

Device Guard

This is essentially an application whitelisting feature that looks for signed applications from vendors, the business, or the Windows App store. As a result, this functionality will greatly enhance the mitigation of zero-day vulnerabilities. Device Guard can use hardware technology and virtualization to isolate that decision-making function from the rest of the Windows operating system, which helps provide protection from attackers or malware that managed to gain full system privilege. Traditional antivirus solutions will be able to depend on Device Guard to help block executable and script-based malware, while antivirus will continue to protect the areas that Device Guard does not such as Java. The enterprise administrators are in control of what sources Device Guard considers trustworthy allowing customization that fits the business’ needs.

Windows Hello

With Windows Hello, users can login or authenticate to their device just by sitting down in front of a device with a compatible camera that uses facial recognition. Windows Hello also works with other biometric components such as iris-scanning or fingerprint-scanning. This effectively eliminates the need to store a password on the device. In independent testing, technology bloggers arranged for 6 sets of identical twins to attempt to thwart the login to a Windows 10 operating system with the use of facial recognition by having the unregistered twin attempt to login in his or her sibling’s place. All 6 attempts failed. The camera technology used for facial or ocular recognition requires infrared cameras, so as to not be easily fooled by a picture. There are multiple vendors who have manufactured devices that support this technology.

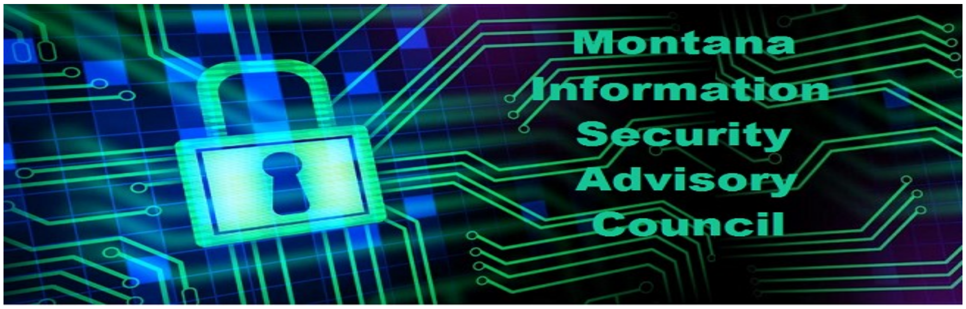
Windows Passport

Where Windows Hello authenticates you to the device, Windows Passport authenticates you to applications and websites through the use of biometrics. Instead of using the traditional userID and password schema, Passport uses a public/private key pair. The private key is stored on the device, and the application or website receives your public key, which is used to request the private key. To ensure the end-user is in control of the device, Windows Passport requires additional authentication before responding with the private key through the use of personal identification number (PIN) or the use of Windows Hello authentication.

Enterprise Data Protection

This feature has yet to be released for the Enterprise version, but the idea is simple: containerization and encryption of files. Administrators will be able to differentiate the origins and locations of business documentation versus personal documents, so that the business documents are protected throughout their lifecycle.

Meeting Highlights of the Montana Information Security Advisory Council Meeting & Preview of the Upcoming Meeting



Meeting highlights from October 21, 2015

The Council reviewed POL-Information Security Policy which merged the five core security policies and incorporated existing appendices A, B, and C along with the new Appendix D into the policy. Full documents can be found on the [MT-ISAC website]() and are being added to the MOM site.

The Council also reviewed the draft DOA-Security Policy which can be used as a template for agencies should they want to state that they will follow the Enterprise Security Policy.

Council voted to rescind 28 Enterprise Security Policies/Standards/Procedures. Each of the 28 documents were approved in September by the Council to be merged into POL-Information Security Policy – Appendix A.

The survey on workgroup creation was reviewed and the Council voted to form two working groups at this time:

Best Practices—Lynne Pizzini, Chair.

Assessment—Lynne Pizzini, Chair.

Situational Awareness—Bryan Costigan, Chair. _*This workgroup was created at the August MT-ISAC meeting_.

Margaret Kauska gave an update on the Joint Task Force on Fraud and Identity Theft.

In the current events segment of the meeting, Sean Rivera spoke on new security technology that is part of Windows 10.

Governor Steve Bullock stopped by to personally thank the Council members as well as security representatives who attend the MT-ISAC meetings for their work and involvement.

The December MT-ISAC meeting will be held during the IT Conference on Monday, December 7th from 1-3 pm in the Natatorium at the Red Lion Colonial Inn in Helena.

For more information, visit the [MT-ISAC website]().

Security Awareness 2015 Events

Focus on Mobile Devices

- Nov 18, 2015 - 11:00-1:00 at DLI's TSD Conference Room
  2550 Prospect Ave

Focus on Phishing

- Dec 1, 2015 - 9:30—12:00 at COR EOC Conference Room
  5 S Last Chance Gulch
- Dec 15, 2015 - 9:30—12:00 at DPHHS Sanders Room 107
  111 N Sanders St

Check [Montana Information Security]() for the latest event schedule and don't forget to come see us at the [Montana IT Conference]() December 7-10, 2015

Security Training News

SANS Securing the Human End User Training

SANS has released an enhancement to the “Breakout Report” which is part of the “Summary Reports” in the SANS Virtual Learning Environment (VLE).

Overview of Release:

- For multi-product accounts, you will need to select the "*Managing License*" tab for the applicable product you want for the "*Breakout Report*"
- The reporting enhancement release will allow the "*Breakout Report*" to show each training program category as a separate report for multiple training product accounts.
- In each product specific report, the "Started" and "Completed" dates for Users will show according to the applicable training product.

For additional information on this release, please visit: https://www.securingthehuman.org/vle_help/blog/2015/09/30/breakout-report-enhancement-release

The Enterprise Security Program (ESP) is available to help with your security training planning and implementation. To request assistance with SANS administration or reporting, please open a case with the SITSD Service Desk at 444-2000 or online.

FREE Security Awareness Training

Who doesn’t like free? The SANS Securing the Human training is available free of charge to all state agencies. Licenses are also available to local governments and the university system through the state contract at a minimal change. But we recognize that budgets are tight everywhere, so when we heard about the PhishMe CBFree security awareness training, we had to check it out. It has 12 modules that cover the basics of user security awareness. Each module takes about five minutes to complete and has about five minutes of additional quiz material about the module. And did we mention it’s free? To learn more go to: http://phishme.com/resources/cbfree-computer-based-training/

State and Local Cybersecurity: A Guide to Federal Resources

Virtual Event — November 12, 2015 11:00– 2:00 ET

Watch from your computer as a panel of cybersecurity experts from NIST, GSA, and DHS provide state and local officials with a better understanding of how to take full advantage of NIST, FedRAMP, and CDM programs. Registration is FREE for government and military personnel. More information and registration.

Reinventing Cybersecurity Training

Virtual Event—November 4, 2015 3:00 ET

A case study in what works and what doesn’t when it comes to security awareness training. Registration
(Password: 7av$#2StEThe)

For more security training and awareness resources, check out the Security Training Resources page and watch for more information here each month.

MDM continued from page 1

manage those devices. As the weeks progressed, more agencies started testing in the pilot phase. Around the first part of October, all agencies were notified that they can start testing the platform and SITSD has been working with them on getting their environments set up.

The EMM platform by AirWatch provides for several different potential solutions that agencies and State of Montana employees may want for their mobile device. The MDM solution provides a single interface for the agency administrators to manage their environment, their users, and the mobile devices of the users. The email management solution allows employees secure access to their State of Montana email, calendar and contacts. The EMM platform also provides solutions to provide containerized applications (including a browser) and content that are isolated on the mobile device from rest on the employee's data on the mobile device.

To provide more information on the AirWatch EMM solutions, SITSD has invited members of the AirWatch team to the 2015 Montana Government IT Conference. They will have a booth at the conference and will be presenting a technical session at the conference on Wednesday, December 9th at 3:00 pm. The title of technical session is Evaluating BYOD and Corporate Device Connectivity.

Please contact Ken Spracklen (kspracklen@mt.gov 406-444-2639) for additional information on the AirWatch EMM solution.

Social Media? Oh, Yeah!

Working in information security, a lot of us have reservations about using social media sites like Facebook, Twitter, Instagram, YouTube, and others. In a few months our focus topic will be all about using social media safely, but in the meantime, we wanted to let you know that Information Systems Security Office and Enterprise Security Program are now on Facebook and Twitter. If you are, too, like our Facebook page: State of Montana Information Security and follow us on Twitter: @MontanaSecurity for more security news, tips, and event announcements.

Montana Government IT Conference Preview

The 12th Annual Montana Government IT Conference will be held December 7-11, 2015 in Helena. Again this year there will be a full track focused on information security, plus a half day cyber security tabletop exercise facilitated by the Department of Homeland Security (DHS).

On Tuesday, December 8th the Information Systems Security Office (ISSO) will have a booth at the trade show. Come by to pick up informational handouts, learn more about our services, play security trivia, and get your picture drawn by a caricature artist.

The sessions in the "Securing Montana's Future" will all be about information security with a mix of in-house presentations, outside speakers, and panel discussions.

On Wednesday, December 9th there will be four security sessions:

- Digital Security
- Creating Effective Security Training and Awareness Programs
- What Is Splunk and What Can It Do For Me
- Digital Forensics (Panel)

The Thursday, December 10th schedule includes four more security sessions:

- Starting with Security
- Source Control Best Practices
- Physical Points of Intrusion
- Introduction to System Security Plans and Risk Assessments (Panel)

On Friday, December 11th the conference will wind up with a cyber security tabletop exercise. This exercise was very well-received in 2014 so we're bringing it back with a new scenario. What is the scenario, you ask? You'll have to come to the exercise to find out but we promise it will be interesting and educational.

In addition to the sessions in the security track, Bryan Seely, a world famous cyber security expert and hacker, will be doing the general session keynote on Thursday morning. Of course, there will be many other sessions and items of interest, so register today!

http://itconference.mt.gov/

Focus continued from page 1

horrible – it's "just" removal of the bad app and a factory reset – it's often difficult to detect an infected phone and mobile phones have some of the same inherent risks as a USB drive. Plug an infected phone into your computer and you've just spread the malware. No longer does a cybercriminal need to access the network to infect it. He can infect the device of an employee and the employee will spread the infection.

Last, let's not forget the low tech and all too common problem of losing devices. Small devices are great because we take them everywhere. But it's also easy to leave them somewhere or have them drop out of our pockets and bags without us noticing. Losing an unlocked and unencrypted device is like dropping a file folder full of information on the street for a stranger to pick up and read.

Here are some steps you can take to protect yourself when using mobile devices:

* Update and patch your device and the apps on it regularly. If your phone is old and no longer supported, consider replacing it. When researching new devices take into consideration which manufacturers are more reliable about regular updates.

* Protect your device with a strong password or passcode. Use encryption when possible to protect the information stored on the device.

* Use caution when installing apps on your device. Download apps from trusted manufacturer's app store, or sources like the Apple Store, Google Play, Amazon, your wireless carrier's store. If your phone is used for work, follow your organization's policy about installing apps, which may include only installing apps from the organization app store or getting approval prior to installing an app.

* If you are installing an app, pay attention to the permissions requested by the app. If the permissions seem excessive – like the ability to copy your contacts or access your photos and email – consider forgoing the app and trying to find another one with similar functionality that would be less intrusive.

* Backup your mobile device on a regular basis. You're doing that with your computer, right? So why aren't you doing it with the little computer in your pocket?

* Install antivirus on your device and keep it updated with the latest version.

* Turn off any functionality that automatically executes files or auto-plays videos.

* Never jailbreak or hack your own device. Not only will this void most support, but it may cause built in security features to no longer work.

* When using your device to surf the internet, remember that malicious sites may infect your mobile device just as they do your desktop.

* Watch out for phishing attempts in your email on your device and also in text messages. If something looks suspicious or too good to be true, just delete it.

* Be careful using Wi-Fi. Consider disabling the function that automatically connects to available Wi-Fi networks or disable Wi-Fi except when you need to use it. If you're using public Wi-Fi, use a VPN to provide protection. NEVER conduct business, do your banking, or shop over public Wi-Fi.

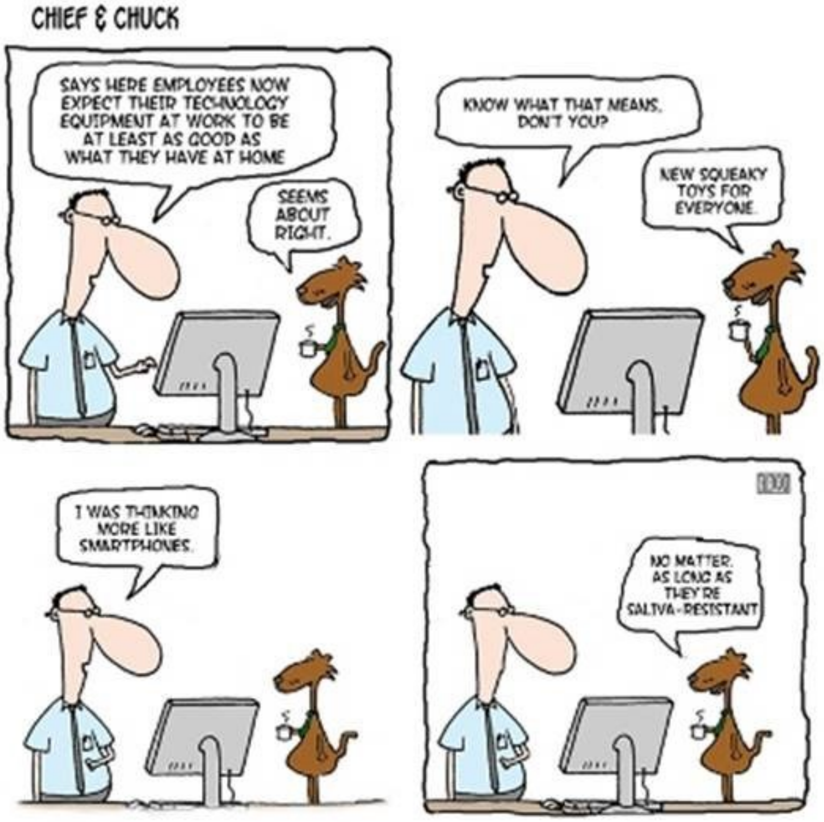
* Bluetooth capabilities are also an entry point for hackers. Disable Bluetooth unless you need it.

* Do not access or store work email or other information from your organization on your mobile device unless you have been authorized and are using approved software.

* Consider enabling remote wiping on your device. If the device is ever lost or stolen you can erase all of your information to prevent it from being stolen.

* Finally, when you're replacing your device, make sure to wipe all data before disposing of it. For mobile phones, remove the SIM and any memory cards from the device.

Mobile devices help us to stay in touch, be more productive, share, and communicate with co-workers, family, and friends. Protecting your device allows us to do all that more securely.


CHIEF & CHUCK
SAYS HERE EMPLOYEES NOW EXPECT THEIR TECHNOLOGY EQUIPMENT AT WORK TO BE AT LEAST AS GOOD AS WHAT THEY HAVE AT HOME
SEEMS ABOUT RIGHT.
KNOW WHAT THAT MEANS, DON'T YOU?
NEW SQUEAKY TOYS FOR EVERYONE.
I WAS THINKING MORE LIKE SMARTPHONES.
NO MATTER. AS LONG AS THEY'RE SALIVA-RESISTANT.

News You Can Use

Focusing on Mobile Devices

2015 Mobile Threats: Ransomware and Data Leaks Run Rampant

The more mobile devices are used the more attractive a target they become for ransomware, unwanted software, and data theft.

Manufacturers Fail to Eliminate Vulnerabilities On Mobile Devices

Security updates for Android devices has left 88% of smartphones and tablets vulnerable to security flaws over the past four years.

Scientists Study Nomophobia—Fear of Being Without a Mobile Phone

An interesting read about our dependence on mobile phones.

SECURITY CAT
NOTICED THAT YOU ARE USING A VPN TO CONNECT TO PUBLIC WIFI AND THAT'S PURRRRRRRFECT
SAC the security awareness COMPANY
© 2014 THE SECURITY AWARENESS COMPANY

Security Quick Tip

Protect your mobile phone just like you would your computer:

- **Use a strong passcode to lock your phone.**
- **Be careful about the apps you install.**
- **Use antivirus software.**

For more security tips, news, advisories, and resources visit the Montana Information Security website, find us on Facebook, or follow us on Twitter.

http://sitsd.mt.gov/MontanaInformationSecurity

State of Montana Information Security

@MontanaSecurity

Contact Us:

Enterprise Security Program

Lynne Pizzini, CISO and Deputy Chief Information Officer

Joe Frohlich, Enterprise Security Manager